BURSOR & FISHER, P.A.
Sarah N. Westcot (State Bar No. 264916)
701 Brickell Avenue, Suite 2100
Miami, FL 33131
Telephone: (305) 330-5512
E-mail: swestcot@bursor.com

Counsel for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

V.R., individually and on behalf of all others similarly situated,

Plaintiff,

v.

LINKEDIN CORPORATION,

Defendant.

Case No. 5:24-cv-07399-EJD

FIRST AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff V.R. ("Plaintiff") brings this class action complaint on behalf of herself and all other persons similarly situated (the "Class Members") against Defendant LinkedIn Corporation ("LinkedIn" or "Defendant"). Plaintiff brings this action based on personal knowledge of the facts pertaining to herself, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1. Plaintiff brings this suit on behalf of all LinkedIn users who live in the United States and who scheduled an urgent care medical appointment through the website www.citymd.com (the "Website"). The Website is owned and operated by Village Practice Management Company, LLC d/b/a CityMD ("CityMD").

2. Patients trust healthcare providers to safeguard their information. Moreover, such information is protected by state and federal law. When booking medical appointments online, Patients reasonably expect the sensitive and legally protected information related to their appointment will remain confidential and protected from third parties. Being able to trust that their health information is secure is essential to upholding patient rights and the integrity of our healthcare system.

3. Health information is incredibly valuable to online advertising companies. Despite the legal protections afforded to this sensitive information, advertising companies go to great lengths to intercept such information to use in their targeted advertising campaigns.

4. Unbeknownst to Plaintiff and members of the putative class, LinkedIn intentionally intercepted these sensitive and confidential communications, including the location and time of their appointment, their gender, and the type of appointment they were seeking treatment for (*see* Figures 2–5). LinkedIn failed to receive consent for these interceptions, and thereby engaged in conduct that expressly contravened its own terms and representations.

5. LinkedIn develops, owns, and operates "the world's largest professional network with more than 1 billion members in more than 200 countries and territories worldwide."[1]

[1] LINKEDIN, ABOUT, https://about.linkedin.com/?trk=homepage-basic_directory_aboutUrl.

LinkedIn is also an advertising company that touts its ability to deliver targeted marketing to specific users.

6. Defendant intercepted this confidential information for target advertising purposes. Plaintiff brings this action for legal and equitable remedies resulting from these illegal acts.

PARTIES

7. Plaintiff V.R. is domiciled in Brooklyn, New York. Plaintiff maintained an active LinkedIn account at all relevant times when booking a medical appointment on the Website. When Plaintiff created her LinkedIn account she agreed to LinkedIn's User Agreement, which provides that "You and LinkedIn agree that the laws of the State of California, U.S.A….shall exclusively govern any dispute relating to this Contract and/or the Services."[2] LinkedIn's "Services," includes those related to its software code known as the LinkedIn Insight Tag.[3]

8. In or around August 9, 2024, Plaintiff scheduled a medical appointment through the Website. When booking her appointment, Plaintiff selected a CityMD location, a time, who she was booking an appointment for, and why she was booking the appointment. Unbeknownst to Plaintiff, LinkedIn was tracking her private activity on CityMD's Website using the LinkedIn Insight Tag. LinkedIn used this software to track Plaintiff and intercept her communications with CityMD, including communications that contained confidential information related to her medical appointment. LinkedIn never received consent from Plaintiff or received permission to track or sell her data to advertisers. LinkedIn's acts and practices, as described herein, are an egregious breach of Plaintiff's privacy.

9. Defendant LinkedIn Corporation is a Delaware corporation with its principal place of business located in Sunnyvale, California. Defendant LinkedIn at all times knew that the incorporation of its software onto the CityMD Website would result in its interception of confidential medical information. Defendant LinkedIn, as the creator of its software and the LinkedIn Insight Tag, knew that it intercepted users' interactions on the Website that incorporated its technology. Defendant LinkedIn is well aware of the dangers of incorporating such technology

[2] LINKEDIN, USER AGREEMENT, https://www.linkedin.com/legal/user-agreement#dispute

[3] *Id.*

on websites that offer medical and health services but continues to do so. LinkedIn intends to intercept this protected and sensitive health data due to the value it holds for targeted advertising purposes. LinkedIn's User Agreement and Privacy Policy both fail to inform LinkedIn account holders that LinkedIn may acquire their confidential medical information when they interact with healthcare providers or covered entity websites and applications. LinkedIn does not obtain consent from its account holders prior to intercepting their confidential medical information nor does it reject or delete confidential medical information that it intercepts through the LinkedIn Insight Tag. Instead, LinkedIn incorporates this data into its advertising machinery for its own independent purposes.

JURISDICTION AND VENUE

10. This Court has subject-matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A), as amended by the Class Action Fairness Act of 2005 ("CAFA"),because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 members of the putative class, and Plaintiff, as well as most members of the proposed class, are citizens of different states than Defendant.

11. This Court has personal jurisdiction over Defendant because Defendant resides in California, Plaintiff submits to the jurisdiction of the Court, and because Defendant, at all times relevant hereto, has systematically and continually conducted, and continues to conduct, business in California.

12. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because Defendant conducts business in this District and throughout the State of California and its principal place of business is in this District.

FACTUAL BACKGROUND

A. Background of the California Information Privacy Act ("CIPA")

13. The CIPA prohibits "any person" from "willfully and without the consent of all parties to the communication … read[ing], or attempt[ing] to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or

attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned[.]" § 631(a).

14. To establish liability under California Penal Code Section 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, or contrivance, or in any other manner," does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> *Or*
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable, or is being sent from, or received at any place within this state,
>
> *Or*
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

15. Section 631(a)'s applicability is not limited to phone lines, but also applies to "new technologies" such as computers, the internet, and email. *See Matera v. Google Inc*., 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (the CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc*., 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006) (the CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 607–08 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' internet browsing history).

16. Plaintiff and Class Members may seek injunctive relief and statutory damages of $5,000 per violation under the CIPA. Cal. Penal Code § 637.2.

B. LinkedIn's Platform and Business Tools

17. LinkedIn markets itself as "the world's largest professional network on the internet[.]"[4] But LinkedIn is no longer simply a tool to help users find jobs or expand their professional network. LinkedIn has moved into the marketing and advertising space and boasts of its ability to allow potential advertisers to "[r]each 1 billion+ professionals around the world" via its Marketing Solutions services.[5] Recently, LinkedIn was projected as being responsible for "roughly 0.9 percent of the global ad revenue" which included approximately $5.91 billion in advertising revenue in 2022.[6]

18. According to LinkedIn, "[t]argeting is a foundational element of running a successful advertising campaign — [g]etting your targeting right leads to higher engagement, and ultimately, higher conversion rates." [7] Targeting refers to ensuring that advertisements are targeted to, and appear in front of, the target demographic for an advertisement. To that end, LinkedIn's Marketing Solutions services allow potential advertisers to "[b]uild strategic campaigns" targeting specific users.[8] LinkedIn's "marketing solutions allow advertisers to select specific characteristics to help them reach their ideal audience. The ads [users] see on LinkedIn are then targeted to provide content relevant to [the users]."[9]

19. As a result of its activities and operation of the LinkedIn Insight Tag, LinkedIn is able to make extremely personal inferences about individuals' demographics, intent, behavior, engagement, interests, buying decisions, and more.[10]

---

[4] LINKEDIN, WHAT IS LINKEDIN AND HOW CAN I USE IT?, https://www.linkedin.com/help/linkedin/answer/a548441#.

[5] LINKEDIN, MARKETING SOLUTIONS, https://business.linkedin.com/marketing-solutions.

[6] Valentina Dencheva, *LinkedIn annual ad revenue 2017-2027*, STATISTA (Dec. 12, 2023), https://www.statista.com/statistics/275933/linkedins-advertising-revenue.

[7] LINKEDIN, REACH YOUR AUDIENCE: TARGETING ON LINKEDIN, p.3, https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/resources/pdfs/linkedin-targeting-playbook-v3.pdf.

[8] LINKEDIN, *supra* note 5.

[9] LINKEDIN, LINKEDIN ADS AND MARKETING SOLUTIONS, https://www.linkedin.com/help/lms/answer/a421454.

[10] *See* LINKEDIN, MARKETING SOLUTIONS, https://business.linkedin.com/marketing-solutions/audience ("Target audiences through demographic marketing[,]" "Zero in on intent,

20. The personal information and communications obtained by LinkedIn are used to fuel various services offered via LinkedIn's Marketing Solutions including Ad Targeting, Matched Audiences, Audience Expansion, and LinkedIn Audience Network.[11]

21. Such information is extremely valuable to marketers and advertisers because the inferences derived from users' personal information and communications allows marketers and advertisers, including healthcare providers and insurance companies, to target potential customers.[12]

22. For example, through the use of LinkedIn's Audience Network, marketers and advertisers are able to expand their reach and advertise on sites other than LinkedIn to "reach millions of professionals across multiple touchpoints."[13] According to Broc Munro of Microsoft, "[w]e gravitate towards social platforms like LinkedIn to achieve more targeted marketing engagement. However, we know that our audiences don't spend all their time on social media. LinkedIn Audience Network enables us to expand our reach to trusted sites while still respecting our audience targeting. This increases the impact of our advertising."[14]

---

behavior, engagement, interests, and more[,]" and "Reach the LinkedIn audience involved in the buying decision").

[11] *See id.*

[12] LINKEDIN, PRIVACY POLICY, https://www.linkedin.com/legal/privacy-policy ("We serve you tailored ads both on and off our Services. We offer you choices regarding personalized ads, but you cannot opt-out of seeing other ads."); LINKEDIN, ACCOUNT TARGETING, https://business.linkedin.com/marketing-solutions/ad-targeting ("Target your ideal customer based on traits like their job title, company name or industry, and by professional or personal interests"); LINKEDIN, EXAMPLES OF TRENDING AND BEST-IN-CLASS HEALTHCARE CAMPAIGNS AND CONTENT, p.6, https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-microsite/resources/lkin-lms-sales-healthcare-campaigns-trending-content-Jan2023.pdf ("BD zeroed in on the end-benefit with a 30 second video introducing their PIVO needle-free blood collection device to potential customers."); LINKEDIN, HEALTHCARE SOCIAL MEDIA STRATEGIES FOR 2023, p.1, https://business.linkedin.com/content/dam/me/business/en-us/marketing-solutions/healthcare-microsite/resources/hc-social-media-trends.pdf (listing "potential customers" as "Common audiences" for insurance sector).

[13] LINKEDIN, ACCOUNT TARGETING, https://business.linkedin.com/marketing-solutions/ad-targeting.

[14] LINKEDIN, LINKEDIN AUDIENCE NETWORK, https://business.linkedin.com/marketing-solutions/native-advertising/linkedin-audience-network.

23. In July 2022, "LinkedIn Marketing Solutions surpassed $5 billion in annual revenue[.]"[15] That figure is "expected to further grow to reach 10.35 billion U.S. dollars by 2027."[16]

24. According to LinkedIn, the LinkedIn Insight Tag is "[a] simple code snippet added to [a] website [that] can help you optimize your campaigns, retarget your website visitors, and learn more about your audiences."[17] LinkedIn represents that the LinkedIn Insight Tag "enable[s] in-depth campaign reporting and unlock[s] valuable insights about your website visitors."[18]

25. LinkedIn's current iteration of its Insight Tag is a JavaScript-based code which allows for the installation of its software.[19] A critical feature allows the LinkedIn Insight Tag to track users, even when third-party cookies are blocked.[20] LinkedIn "recommend[s] using the JavaScript-based Insight Tag or Conversions API" because third-party cookie settings are being deprecated across the industry.[21] Embedding the JavaScript as a first-party cookie causes users' browsers to treat the LinkedIn Insight Tag as though it is offered by the website being visited, rather than by LinkedIn. Doing so ensures that the third-party cookie-blocking functions of modern web browsers do not prevent LinkedIn from collecting data through its software.[22] Instead, the LinkedIn Insight Tag is shielded with the same privacy exemptions offered to first-party cookies.

---

[15] *LinkedIn Business Highlights from Microsoft's FY22 Q4 Earnings*, LINKEDIN PRESSROOM (July 25, 2022), https://news.linkedin.com/2022/july/linkedin-business-highlights-from-microsoft-s-fy22-q4earnings#:~:text=And%20LinkedIn%20Marketing%20Solutions%20surpassed,revenue%20for%20the%20first%20time.

[16] Dencheva, *supra* note 6.

[17] LINKEDIN, INSIGHT TAG, https://business.linkedin.com/marketing-solutions/insight-tag.

[18] LINKEDIN, LINKEDIN INSIGHT TAG FAQS, https://www.linkedin.com/help/lms/answer/a427660.

[19] LINKEDIN, *supra* note 17.

[20] *Id.* ("It's important for advertisers to prepare for these changes by switching to JavaScript tags and enabling 'enhanced conversion tracking' in the Insight Tag settings to continue capturing signals where 3rd party cookies are blocked.").

[21] *See id.*

[22] *See id.*

26. When a user who has signed in to LinkedIn (even if the user subsequently logs out) is browsing a website where the LinkedIn Insight Tag has been embedded, an HTTP request is sent using cookies, which includes information about the user's actions on the website.

27. These cookies also include data that differentiate users from one another and can be used to link the data collected to the user's LinkedIn profile.

28. The HTTP request about an individual who has previously signed into LinkedIn includes requests from the "li_sugr" and "lms_ads" cookies. Each of these cookies are used by LinkedIn "to identify LinkedIn Members off LinkedIn" for advertising purposes.[23]

29. For example, the "li_sugr" cookie is "[u]sed to make a probabilistic match of a user's identity."[24] Similarly, the "lms_ads" cookie is "[u]sed to identify LinkedIn Members off LinkedIn for advertising."[25]

30. A LinkedIn profile contains information including an individual's first and last name, place of work, contact information, and other personal details. Based on information it obtains through the LinkedIn Insight Tag, Defendant LinkedIn is able to target its account holders for advertising.

31. LinkedIn never receives consent from users to intercept and collect electronic communications containing their sensitive and unlawfully disclosed information. In fact, LinkedIn expressly warrants the opposite.

32. When first signing up, a user agrees to the User Agreement.[26] By using or continuing to use LinkedIn's Services, users agree to two additional agreements: the Privacy Policy[27] and the Cookie Policy.[28]

---

[23] LINKEDIN, LINKEDIN COOKIE TABLE, https://www.linkedin.com/legal/l/cookie-table.

[24] *See id.*

[25] *See id.*

[26] LINKEDIN, USER AGREEMENT, https://www.linkedin.com/legal/user-agreement.

[27] LINKEDIN, PRIVACY POLICY, https://www.linkedin.com/legal/privacy-policy.

[28] LINKEDIN, COOKIE POLICY, https://www.linkedin.com/legal/cookie-policy.

33. LinkedIn's Privacy Policy begins by stating that "LinkedIn's mission is to connect the world's professionals . . . . Central to this mission is our commitment to be transparent about the data we collect about you, how it is used and with whom it is shared."[29]

34. The Privacy Policy goes on to describe what data LinkedIn collects from various sources, including cookies and similar technologies.[30] LinkedIn states "we use cookies and similar technologies (e.g., pixels and ad tags) to collect data (e.g., device IDs) to recognize you and your device(s) on, off and across different services and devices where you have engaged with our Services. We also allow some others to use cookies as described in our Cookie Policy."[31]

35. However, LinkedIn offers an express representation: "**We will only collect and process personal data about you where we have lawful bases.**"[32]

36. Despite this explicit representation, LinkedIn intentionally intercepts and receives sensitive and unlawfully disclosed information in violation of state and federal privacy laws.

37. Users never choose to provide sensitive information to LinkedIn because, among other reasons, they never know whether a particular website uses the LinkedIn Insight Tag, and, if so, what sensitive personal data it collects.

C. How LinkedIn Intercepted Plaintiff's and Class Members' Protected Health Information

38. CityMD is a provider of accessible healthcare services that permits patients to schedule appointments at their brick-and-mortar locations through its Website. Upon entering the Website, CityMD warrants that it will help patients receive "care that can't wait."

39. To begin, patients browse available CityMD locations and select which location they would like to book an appointment at. *See* Figure 1.

[29] LINKEDIN, PRIVACY POLICY, https://www.linkedin.com/legal/privacy-policy.

[30] *Id.*

[31] *Id.*

[32] *Id.* (emphasis added).

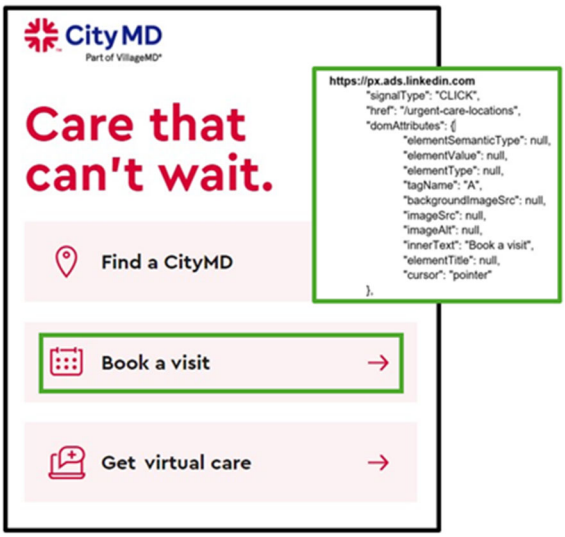

Figure 1: Screenshot of CityMD Website with pixel interceptions overlayed (confirmable with developer tools)

40. Unbeknownst to consumers, LinkedIn was tracking their activity the moment they entered the CityMD Website.

41. For example, the LinkedIn Insight Tag was embedded on the Website, which allowed LinkedIn to intercept and record "click" events. Click events detail information about which page on the Website the patient was viewing as well as the selections they were making. LinkedIn intercepts information including the patient's appointment time, who the appointment was for, why they were booking the appointment, and their gender. *See* Figures 1–5.

Figure 2: Screenshot of CityMD Website with pixel interceptions overlayed (confirmable with developer tools)

Figure 3: Screenshot of CityMD Website with pixel interceptions overlayed (confirmable with developer tools)

Figure 4: Screenshot of CityMD Website with pixel interceptions overlayed (confirmable with developer tools)

Figure 5: Screenshot of CityMD Website with pixel interceptions overlayed (confirmable with developer tools)

42. Through the LinkedIn Insight Tag, Defendant intercepted consumers confidential information related to their medical appointments in order to monetize that data for targeted advertising.

43. As shown in Figures 2 through 5, LinkedIn intercepts several pieces of confidential information, including the location and time of their appointment, their gender, and the type of appointment they were seeking treatment for.

44. These interceptions also included the li_sugr and lms_ads cookies, which LinkedIn utilizes to identify its account holders for targeted advertising.

45. LinkedIn incorporated the information it intercepted from the CityMD Website into its marketing tools to fuel its targeted advertising service.

46. Plaintiff never consented, agreed, authorized, or otherwise permitted LinkedIn to intercept her confidential health information.

47. By law, Plaintiff is entitled to privacy in her protected health information and confidential communications. LinkedIn deprived Plaintiff of her privacy rights when it implemented a system that surreptitiously tracked and recorded Plaintiff's and other online

consumers' confidential communications, personally identifiable information, and protected health information.

D. LinkedIn's Conduct Violates Federal and State Privacy Laws

48. Patient healthcare information is protected by federal law under the Health Insurance Portability and Accountability Act ("HIPAA") and its implementing regulations, which are promulgated by the Department of Health and Human Services ("HHS").

49. Under federal law, PII, non-public medical information about a patient, potential patient, or household member of a patient may not be disclosed without the patient's express written authorization.[33]

50. Guidance from HHS provides that patient status alone is protected by HIPAA.

51. HIPAA's Privacy Rule defines "individually identifiable health information" ("IIHI") as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

52. The Privacy Rule broadly defines protected health information as IIHI that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

53. Under the HIPAA de-identification rule, "health information is not individually identifiable only if": (i) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods

[33] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

and results of the analysis that justify such determination'" or (ii) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed:

A. Names;
…
H. Medical record numbers;
…
J. Account numbers;
…
M. Device identifiers and serial numbers;
N. Web Universal Resource Locators (URLs);
O. Internet Protocol (IP) address numbers; … and
P. Any other unique identifying number, characteristic, or code… and" the covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."[34]

54. Even the fact that an individual is receiving a medical service, i.e., is a patient of a particular entity, can be PHI. Guidance from HHS confirms as much:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data. … If such information was listed with health condition, healthcare provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[35]

55. HHS has previously instructed that patient status is protected by the HIPAA Privacy Rule:

(a) "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);

(b) "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications,"

[34] *See* 45 C.F.R. § 160.514.

[35] Office for Civil Rights, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule at 5 (emphasis added) (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/Deidentification/hhs_deid_guidance.pdf.

which includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002);

(c) It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013); and

(d) The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

56. HHS has issued numerous bulletins informing covered entities and their business associates that the use of online tracking technology, like the LinkedIn Insight Tag, can lead to violations of the HIPAA Privacy Rule.[36]

57. Tracking technology vendors like LinkedIn are considered business associates under HIPAA if they provide services to healthcare providers and receive or maintain PHI, like LinkedIn does:

> Furthermore, tracking technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (e.g. healthcare operations) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI. In these circumstances, regulated entities must ensure that the disclosures made to such vendors are permitted by the Privacy Rule and enter into a business associate agreement (BAA) with these tracking technology vendors to ensure that PHI is protected in accordance with the HIPAA Rules. For example, if an individual makes an appointment through the website of a covered health clinic for health services and that website uses third party tracking technologies, then

[36] HHS.gov, HHS Office of Civil Rights Issue Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information (Dec. 1, 2022), https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-onrequirements-under-hipaa-for-online-tracking-technologies.html.

> the website might automatically transmit information regarding the appointment and the individual's IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate and a BAA is required.

58. HIPAA applies to healthcare providers' webpages with tracking technologies even outside the patient portal:

> Tracking on unauthenticated webpages
>
> [T]racking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal … [and pages] that address[] specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a healthcare provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.

59. And no PHI may be disclosed to tracking technology vendors, like LinkedIn, unless the healthcare provider has properly notified its website users and entered into a business associate agreement with the vendor:

> Regulated entities may identify the use of tracking technologies in their website or mobile app's privacy policy, notice, or terms and conditions of use. However, the Privacy Rule does not permit disclosures of PHI to a tracking technology vendor based solely on a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures. Regulated entities must ensure that all tracking technology vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI.
>
> If there is not an applicable Privacy Rule permission or if the vendor is not a business associate of the regulated entity, then the individual's HIPAA-compliant authorizations are required before the PHI is disclosed to the vendor. Website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do not constitute a valid HIPAA authorization.

> [I]t is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place and requires that there is an applicable Privacy Rule permission for disclosure.

60. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual." The statute states that a "person…shall be considered to have obtained or disclosed individually identifiable health information…if the information is maintained by a covered entity…and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320d-6.

61. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to LinkedIn when it is knowingly obtaining individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

62. California state law is in accord.

63. Plaintiff's and Class Members' information transmitted via the LinkedIn Insight Tag was received in California.

64. California has enacted several laws to protect patients' information. The California Confidentiality of Medical Information Act requires healthcare providers to preserve the confidentiality of patients' medical information and to obtain valid authorization before disclosing a patient's medical information to a third party. Cal. Civ. Code § 56, *et seq*. The California Consumer Privacy Protection Act requires businesses to disclose that they are obtaining medical information for marketing purposes and obtain written consent. Cal. Civ. Code § 1798.91(a)(2), (c). The California Consumer Privacy Act of 2018 requires business to notify consumers when they collect sensitive personal information, including medical information, and the purposes of the collection and use of that information. Cal. Civ. Code § 1798.100 *et seq*.

65. LinkedIn's conduct in this action violates each of these California laws or involves LinkedIn's knowing participation with healthcare entities in violating these California laws.

CLASS ALLEGATIONS

66. **Class Definition:** Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of all LinkedIn account holders in the United States who booked a medical appointment on www.citymd.com (the "Class").

67. Excluded from the Class is Defendant, the officers and directors of the Defendant at all relevant times, members of their immediate families and their legal representatives, heirs, successors, or assigns and any entity in which either Defendant have or had a controlling interest.

68. Plaintiff is a member of the Class she seeks to represent.

69. **Class Period:** The "Class Period" is the time period beginning on the date established by the Court's determination of any applicable statute of limitations, after consideration of any tolling, concealment, and accrual issues, and ending on the date of entry of judgement.

70. Excluded from the Class are Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer, director, or employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, their spouse and immediate family members; and members of the judge's staff.

71. **Numerosity (Fed. R. Civ. P. 23(a)(1)):** Members of the putative Class are so numerous that their individual joinder herein is impracticable. Based on information and Plaintiff's belief, members of the putative Class number in the thousands. The precise number of putative Class Members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Putative Class Members may be notified of the pendency of this action by mail and/or publication through the distribution of Defendant's records.

72. **Commonality and Predominance (Fed. R. Civ. P. 23(a)(2), 23(b)(3)):** Common questions of law and fact exist as to all putative Class Members and predominate over questions affecting only individual Class Members. Common legal and factual questions include, but are not limited to:

(a) Whether LinkedIn's conduct violations the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.*;

(b) Whether LinkedIn's conduct violates the California Invasion of Privacy Act, Cal. Penal Code § 630, *et seq*.;

(c) Whether LinkedIn learned the contents of Plaintiff's and Class Members' communications with CityMD;

(d) Whether LinkedIn used the information it learned from the contents of Plaintiff's and Class Members' communications with CityMD; and

(e) Whether LinkedIn intentionally used an electronic amplifying or recording device to eavesdrop or record Plaintiff's and Class Members' confidential communications with CityMD without the Plaintiff's and Class Members' consent.

73. **Typicality (Fed. R. Civ. P. 23(a)(3)):** Plaintiff's claims are typical of the claims of the members of the Class as all members of the Class are similarly affected by Defendant's wrongful conduct. Plaintiff has no interests antagonistic to the interests of the other members of the Class. Plaintiff and all members of the Class have sustained economic injury arising out of Defendant's violations of statutory law as alleged herein.

74. **Adequacy (Fed. R. Civ. P. 23(a)(4)):** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the putative Class Members she seeks to represent, she has retained counsel competent and experienced in prosecuting class actions, and she intends to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

75. **Superiority (Fed. R. Civ. P. 23(b)(3)):** The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Plaintiff and the putative members of the Class. Each individual Class Member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a

single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims are consistently adjudicated.

76. California law applies to the entirety of the Class. California's substantive laws apply to every member of the Class, regardless of where in the United States the Class member resides. Defendant's own User Agreement explicitly states that "[i]n the unlikely event we end up in a legal dispute . . . you and LinkedIn agree to resolve it in California courts using California law[.]"[37] By choosing California law for the resolution of disputes covered by its User Agreement, LinkedIn concedes that it is appropriate for this Court to apply California law to the instant dispute to all Class Members. Further, California's substantive laws may be constitutionally applied to the claims of Plaintiff and the Class Members under the Due Process Clause, see U.S. Const. amend. XIV, § 1, and the Full Faith and Credit Clause. *See* U.S. Const. art. IV, § 1. California has significant contact, or significant aggregation of contacts, the claims asserted by the Plaintiff and all Class Members thereby creating state interests that ensure that the choice of California state law is not arbitrary or unfair. Defendant's decision to reside in California and avail itself of California's laws, and to engage in the challenged conduct from and emanating out of California, renders the application of California law to the claims herein constitutionally permissible. The application of California laws to the Class is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiff and the proposed Class and California has the greatest interest in applying its laws here.

77. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

[37] LINKEDIN, USER AGREEMENT, note 2.

COUNT I
Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2510, *et seq.*

78. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the Class against Defendant.

79. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

80. The ECPA protects both sending and receipt of communications.

81. The ECPA provides a private right of action to any person whose electronic communications are intercepted. 18 U.S.C. § 2520(a).

82. LinkedIn intentionally intercepted electronic communications that Plaintiff and Class Members exchanged with their healthcare provider through the LinkedIn Insight Tag installed on the CityMD Website.

83. The transmissions of data between Plaintiff and Class Members and their healthcare provider (CityMD) qualify as communications under the ECPA. 18 U.S.C. § 2510(12).

84. LinkedIn contemporaneously acquired Plaintiff's and Class Members' communications with CityMD.

85. The intercepted communications include the contents of Plaintiff's and Class Members' communications relating to appointments with CityMD.

86. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

(a) The cookies LinkedIn used to track Plaintiff's and Class Members' communications;

(b) Plaintiff's and Class Members' browsers;

(c) Plaintiff's and Class Members' computing devices;

(d) LinkedIn's web-servers;

(e) The web-servers of CityMD where the LinkedIn Insight Tag is present; and

(f) The LinkedIn Insight Tag source code LinkedIn deploys to acquire Plaintiff's and Class Members' communications

87. LinkedIn is not a party to Plaintiff's and Class Members' communications with CityMD.

88. LinkedIn receives the content of Plaintiffs' and Class members' communications through the surreptitious redirection of those communications from the Plaintiff's and Class members' computing devices.

89. Plaintiff and Class Members did not consent to LinkedIn's acquisition of their appointment communications with CityMD.

90. LinkedIn did not obtain legal authorization to obtain Plaintiff's and Class Members' communications with CityMD relating to communications with their health providers.

91. LinkedIn did not require CityMD to obtain the lawful rights to share the content of Plaintiff's and Class Members' communications relating to patient appointments.

92. Any purported consent that LinkedIn received from CityMD to obtain the content of Plaintiff's and Class Members' communications was not valid.

93. In acquiring the content of Plaintiff's and Class Members' communications relating to their appointments with CityMD, LinkedIn had a purpose that was tortious, criminal, and designed to violate state constitutional and statutory provisions including:

(a) The unauthorized acquisition of individually identifiable health information is tortious in and of itself regardless of whether the means deployed to acquire the information violates the Wiretap act or any subsequent purpose or use for the acquisition. LinkedIn intentionally committed a tortious act by acquiring individually identifiable health information without authorization to do so.

(b) The unauthorized acquisition of individually identifiable health information is a criminal violation of 42 U.S.C. § 1320d-6 regardless of any subsequent purpose or use of the individually identifiable health information. LinkedIn

intentionally violated 42 U.S.C. 1320d-6 by intentionally acquiring individually identifiable health information without authorization.

(c) A violation of HIPAA, particularly 42 U.S.C. § 1320d-6, which is a criminal offensive punishable by fine or imprisonment with increased penalties where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage [or] personal gain." LinkedIn intentionally violated the enhanced penalty provision of 42 U.S.C. § 1320d-6 by acquiring the individually identifiable health information "with intent to sell transfer or use" it for "commercial advantage [or] personal gain."

(d) A knowing intrusion upon Plaintiffs' and Class members' seclusion; and

(e) Violation of various state health privacy statutes, including but not limited to the California Confidentiality of Medical Information Act; the California Consumer Privacy Protection Act; and the California Consumer Privacy Act.

94. The federal wire fraud statute, 18 U.S.C. § 1343, has four elements: (1) that the defendant voluntarily and intentionally devised a scheme to defraud another out of money or property; (2) that the defendant did so with the intent to defraud; (3) that is was reasonably foreseeable that interstate wire communications would be used; and (4) that interstate wire communications were in fact used. The attempt version of the wire fraud statute provides that "[a]ny person who attempts or conspires to commit any offense under this chapter shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy." 18 U.S.C. § 1349.

95. LinkedIn's scheme or artifice to defraud in this action consists of the false and misleading statements and omissions in its User Agreement and the placement of LinkedIn's JavaScript based code disguising the LinkedIn Insight Tag as a first-party cookie of the patients' healthcare provider (CityMD) rather than a third party cookie from LinkedIn.

96. The "property" involved consists of Plaintiff's and Class Members property rights to the confidentiality of their individually identifiable health information and their right to

determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes and the property rights to determine who has access to their computing devices.

97. LinkedIn acted with the intent to defraud in that it willfully invaded and took Plaintiff's and Class Members' property rights (a) to the confidentiality of their individually identifiable health information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes and (b) to determine who has access to their computing devices.

98. It was reasonably foreseeable to LinkedIn that its scheme and artifice to defraud would involve interstate wire communications and, in fact, interstate wire communications were used in the carrying out of LinkedIn's scheme and artifice to defraud.

99. Courts around the country have uniformly held that a healthcare provider's use of online tracking technology, like the LinkedIn Insight Tag, on its website without patient authorization is actionable in tort or contract or a statutory violation. See *Doe v. Mercy Health*, Case No. A 2002633 (Hamilton County, Ohio); *Doe v. Partners*, Case No. 1984-CV-01651 (Suffolk County, Massachusetts); *Doe v. Sutter Health*, Case No. 34-2019-00258072-CU-BT-GDS (Sacramento County, California); *Doe v. University Hospitals*, Case No. CV-20-9333357 (Cuyahoga County, Ohio); *Doe v. Sutter Health*, Case No. 34-2019-00258072-CU-BT-GDS (Sacramento County, California).

100. As a result of Defendant's violation of the ECPA, Plaintiff and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT II
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 631

101. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the Class against Defendant.

102. The California Invasion of Privacy Act (the "CIPA") is codified at California Penal Code Sections 630 to 638. The CIPA begins with its statement of purpose—namely, that the purpose of the CIPA is to "protect the right of privacy of the people of [California]" from the threat posed by "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications . . ." Cal. Penal Code § 630.

103. A person violates California Penal Code Section 631(a), if:

> by means of any machine, instrument, or contrivance, or in any other manner, [s/he] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [s/he] willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or [s/he] uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained . . .[38]

104. To avoid liability under section 631(a), a defendant must show it had the consent of ***all*** parties to a communication.

105. At all relevant times, LinkedIn tracked and intercepted Plaintiff's and Class Members' internet communications while using www.citymd.com to book a medical appointment. These communications were intercepted without the authorization and consent of Plaintiff and Class Members.

106. Through these interceptions, LinkedIn intended to learn some meaning of the content the visitors requested.

107. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, the LinkedIn Insight Tag fall under the broad catch-all category of "any other manner":

a. The computer codes and programs LinkedIn used to track Plaintiff and Class

[38] Cal. Penal Code § 631(a).

Members' communications while they were navigating www.citymd.com;

b. Plaintiff's and Class Members' browsers;

c. Plaintiff's and Class Members' computing and mobile devices;

d. LinkedIn's web and ad servers;

e. The web and ad servers from which LinkedIn tracked and intercepted Plaintiff's and Class Members' communications while they were using a web browser to access or navigate www.citymd.com;

f. The computer codes and programs used by LinkedIn to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a browser to visit www.citymd.com; and

g. The plan LinkedIn carried out to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser or mobile device to visit www.citymd.com.

108. At all relevant times, LinkedIn, though the LinkedIn Insight Tag, intentionally tapped or made unauthorized connections with the lines of internet communications between Plaintiff and Class Members and the CityMD Website without the consent of all parties to the communication.

109. LinkedIn, willfully and without the consent of Plaintiff and Class Members, read or attempted to read, or learn the contents or meaning of Plaintiff's and Class Members' communications to CityMD while the communications are in transit or passing over any wire, line or able, or were being received at any place within California when it intercepted Plaintiff's and Class Members' communications and data with CityMD.

110. LinkedIn used or attempted to use the communications and information they received through their tracking technology, including to supply advertising services.

111. The patient communication information intercepted through the LinkedIn Insight Tag, such as information related to medical appointments, constituted protected health information.

112. As a result of the above violations, Defendant is liable to Plaintiff and other Class Members in the amount of $5,000 dollars per violation or three times the amount of actual

damages, whichever is greater. Additionally, California Penal Code Section 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages."

113. Under the CIPA, Defendant is also liable for reasonable attorney's fees, and other litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future.

COUNT III
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 632

114. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the Class against Defendant.

115. Cal. Penal Code § 632 prohibits "intentionally and without the consent of all parties to a confidential communication," the "use[] [of] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication."

116. Section 632 defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto[.]"

117. Plaintiff's and Class Members' communications to CityMD, including their sensitive personal and health information, such as why they are booking appointments, were confidential communications for purposes of § 632, because Plaintiff and Class Members had an objectively reasonable expectation of privacy in this data.

118. Plaintiff and Class Members expected their communications to CityMD to be confined to CityMD in part, due to the protected nature of the health information at issue. Plaintiff and Class Members did not expect third parties, like LinkedIn, to secretly eavesdrop upon or record this confidential information and their communications.

119. LinkedIn's tracking technology, i.e., the LinkedIn Insight Tag, are all electronic amplifying or recording devices for purposes of § 632.

120. By contemporaneously intercepting and recording Plaintiff's and Class Members' confidential communications to CityMD through this technology, LinkedIn eavesdropped and/or recorded confidential communications through an electronic amplifying or recording device in violation of § 632 of CIPA.

121. At no time did Plaintiff or Class Members consent to LinkedIn's conduct, nor could they reasonably expect that their communications to CityMD would be overheard or recorded by LinkedIn.

122. LinkedIn utilized Plaintiff's and Class Members' sensitive personal and health information for its own purposes, including for targeted advertising.

123. Plaintiff and Class Members seek statutory damages in accordance with § 637.2(a) which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff and the Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

124. Plaintiff and Class Members have also suffered irreparable injury from these unauthorized acts. Plaintiff's and Class Members' sensitive data has been collected, viewed, accessed, stored, by LinkedIn, have not been destroyed, and due to the continuing threat of such injury, have no adequate remedy at law. Plaintiff and Class Members are accordingly entitled to injunctive relief.

COUNT IV
Invasion of Privacy Under California's Constitution

125. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the Class against Defendant.

126. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion, or interference, including, but not limited to, the right to visit and interact with various

internet sites without being subjected to wiretaps without Plaintiff's and Class Members' knowledge or consent.

127. At all relevant times, by using the LinkedIn Insight Tag to record and communicate patients' personal identifiers alongside their confidential medical communications, Defendant intentionally invaded Plaintiff's and Class Members' privacy rights under the California Constitution.

128. Plaintiff and Class Members had a reasonable expectation that their communications, identities, health information, and other data would remain confidential, and that Defendant would not intercept such information communicated on www.citymd.com.

129. Plaintiff and Class Members did not authorize Defendant to record and transmit Plaintiff's and Class Members' private medical communications alongside their personally identifiable and health information.

130. This invasion of privacy was serious in nature, scope, and impact because it related to patients' private medical communications. Moreover, it constituted an egregious breach of societal norms underlying the privacy right.

131. Accordingly, Plaintiff and Class Members seek all relief available for invasion of privacy under the California Constitution.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief and judgment, as follows:

(a) For a determination that this action is a proper class action;

(b) For an order certifying the Class, naming Plaintiff as representative of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;

(c) For an order declaring that Defendant's conduct violated the statutes referenced herein;

(d) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(e) For an award of compensatory damages, including statutory damages where available, to Plaintiff and the Class Members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial;

(f) For punitive damages, as warranted, in an amount to be determined at trial;

(g) For an order requiring Defendant to disgorge revenues and profits wrongfully obtained;

(h) For prejudgment interest on all amounts awarded;

(i) For injunctive relief as pleaded or as the Court may deem proper;

(j) For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit; and

(k) For an order granting Plaintiff and Class Members such further relief as the Court deems appropriate.

JURY TRIAL DEMANDED

Plaintiff, on behalf of herself and the proposed Class, demands a trial by jury for all of the claims asserted in this Complaint so triable.

Dated: February 12, 2025

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Sarah N. Westcot*
Sarah N. Westcot

Sarah N. Westcot (State Bar No. 264916)
701 Brickell Ave., Suite 2100
Miami, FL 33131-2800
Telephone: (305) 330-5512
Facsimile: (305) 676-9006
Email: swestcot@bursor.com

Counsel for Plaintiff